Contrato No.	ADRES-CTO-868-2023		
Nombre del Contratista y/o Representante Legal	Unión Temporal SOC ADRES 2023		
Nombre del Supervisor y/o Interventor	Guillermo Manuel Benítez Rodriguez	**Teléfono / Extensión**	(57) (1) 4322760 ext. 1724
Dependencia	Dirección de Gestión de Tecnologías de Información y Comunicaciones		
Objeto del Contrato	Prestar el Servicio de Centro de Operaciones de Seguridad para la ADRES (SOC)		
Fecha de Inicio	13/07/2023	**Fecha de Terminación**	31/12/2025

Periodo del Informe de Actividades	**Desde**	1/05/2024	**Hasta**	31/05/2024
Adición y/o Prórroga	No aplica			
Suspensión	No aplica			
Cesión	No aplica			

INFORME PARCIAL DE EJECUCIÓN DE OBLIGACIONES CONTRACTUALES [i]

	Obligación contractual	Actividad desarrollada	Producto y/o Entregables	Alertas, inconvenientes o situaciones especiales que afectan el cumplimiento de la obligación
1	Prestar el servicio de análisis de vulnerabilidades descrito en el numeral 2.1 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye la evaluación de las debilidades o brechas, presentación de los respectivos informes y la construcción de la hoja de ruta con definición de las acciones a seguir para remediar los hallazgos encontrados sobre la infraestructura de TI	El servicio de análisis de vulnerabilidades es por demanda una vez al año: - Para el año 2023 se ejecutó en el mes de octubre. - Para el año 2024 el ejercicio está planeado para realizarse en el mes de septiembre.	N/A	N/A
2	Prestar el servicio de análisis de vulnerabilidades sobre las aplicaciones web descrito en el numeral 2.2 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye la evaluación de las debilidades o brechas, presentación de los respectivos informes y la construcción de la hoja de ruta con definición de las acciones a seguir para remediar los hallazgos encontrados sobre las aplicaciones.	El servicio de análisis de vulnerabilidades sobre las aplicaciones web es por demanda una vez al año: - Para el año 2023 se ejecutó en el mes de octubre. - Para el año 2024 el ejercicio está planeado para realizarse en el mes de septiembre.	N/A	N/A
3	Prestar el servicio de Ethical Hacking descrito en el 2.3 del ANEXO – ESPECIFICACIONES TECNICAS, mediante la realización de ejercicios o pruebas específicas que busquen explotar de manera controlada uno o varios hallazgos encontrados en el análisis de vulnerabilidades.	El servicio de Ethical Hacking es por demanda una vez al año: - Para el año 2023 se ejecutó en el mes de noviembre. - Para el año 2024 el ejercicio está planeado para realizarse en el mes de Octubre.	N/A	N/A
4	Prestar el servicio de Ingeniería Social descrito en el numeral 2.4 del ANEXO – ESPECIFICACIONES TECNICAS, mediante la realización de ejercicios	El servicio de Ingeniería Social es por demanda tres veces al año: -Para el año 2023 los ejercicios se ejecutaron en los meses de septiembre, octubre y noviembre.	N/A	N/A

	controlados y dirigidos al personal de la entidad con el fin de obtener datos confidenciales o infectar los computadores con algún tipo de programa malicioso.	- Para el año 2024 el primer ejercicio se ejecutó en el mes de Marzo, los otros dos ejercicios están planeados para realizarse en los meses de Julio y Septiembre.		
5	Prestar el servicio de monitoreo y correlación de eventos de seguridad en la modalidad 7x24 según lo descrito en el numeral 2.5 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye correlación de eventos, detección, investigación y respuesta ante eventos, incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la ADRES.	A continuación, se relacionan las actividades más relevantes del periodo: • Identificación y atención de eventos de monitoreo el cual corresponde a 2.479. • Identificación y atención de alertas de monitoreo el cual corresponde a 9.242. • Durante el periodo, se bloquearon **850** indicadores de compromiso (IoC): o **Hash – 646** IoCs correspondiente al **76.01**% o **IP – 101** IoCs correspondiente al **11.88**% o **URL/Dominio – 92** IoCs correspondiente al **10.82%** o **Correo/Malware-Phishing – 11** IoCs corresponde al **1.29**% • Se identifican un Top cinco (5) de ataques detectados en la entidad. • Se identifican un Top cinco (5) de usuarios con autenticaciones fallidas. • Se identifican un Top Cuatro (4) de dispositivos con eventos de seguridad. • Elaboración del informe mensual.	• Monitoreo y Correlación de eventos de Seguridad_Mayo_2024.docx • Anexos: o SecurityIncident_by_Events.csv o SecurityIncident_by_IncidentNumber.csv	N/A
6	Prestar el servicio de monitoreo y supervisión de la actividad de bases de datos en la modalidad 5x8 según lo descrito en el numeral 2.6 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye implementación de casos de uso, soporte técnico y mantenimiento de la infraestructura de la solución IMPERVA.	A continuación, se relacionan las actividades más relevante del periodo: • Se llevaron a cabo dos (2) sesiones de trabajo para darle orientación al servicio de monitoreo y supervisión de la actividad de bases de datos. • Se identificaron nuevas bases de datos en las instancias: o Nube Publica - Microsoft Azure: **98** bases de datos en Producción. o Nube Privada – On premise: **390** bases de datos en producción. o Nube Privada – On premise: **30** bases de datos en pruebas. • En la plataforma de IMPERVA DAM se configuran las políticas, quedando de la siguiente manera: - Políticas de seguridad: 69 - Políticas de auditoria: 12 • Se identifican un Top diez (10) de instancias de base de datos que más se alertan. • Monitoreo del estado de Salud del IMPERVA y validación de almacenamiento de la herramienta.	Informe Monitoreo y supervisión de actividad de bases de datos_Mayo_2024.docx • Anexo: Inventario BD.xlsx	N/A
7	Prestar el servicio de Gestión de incidentes en la modalidad 7x24 según lo descrito en el numeral 2.7 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye los procedimientos que permitan reaccionar ante los incidentes de la mejor manera posible, minimizando los daños de los sistemas de información, con diagnósticos eficaces, recolectando las evidencias necesarias y mitigando las causas de los incidentes.	A continuación, se relacionan las actividades más relevantes del periodo: • Durante el periodo en curso se registró un (1) caso de Sentinel documentado y escalado a la entidad. • Se documentaron veintitrés (23) requerimientos por correo y se atendieron según creación de caso por mesa de servicio. • Se enviaron setenta y nueve (79) boletines de seguridad de tipo lite y completos. • Se compartió el análisis de dos (2) posibles casos de suplantación de marca.	Matriz de eventos o incidentes de seguridad - Mayo 2024.xlsx	N/A
8	Prestar el servicio de Gestión de infraestructura de seguridad en la modalidad 5x8 según lo descrito en el numeral 2.8 del ANEXO – ESPECIFICACIONES TECNICAS, con el fin de mejorar el tiempo de respuesta ante incidentes y amenazas de seguridad.	A continuación, se relacionan las actividades más relevantes del periodo: • Para Microsoft Sentinel, en el periodo se gestionó: o Libros: **11** o Conectores de datos: **24** o Reglas de analítica: **37** o Reglas de automatización: **48** o Cuadernos de Estrategia: **17** • Dentro del monitoreo al Azure Monitor se evidencio lo siguiente: o Servidores habilitados para ARC: **89** migrados con éxito. o Maquinas virtuales Azure: **59** migrados con éxito.	Gestión de infraestructura de seguridad_Mayo_2024.docx	N/A

		• Para el Defender for cloud la postura de seguridad quedo en un **67%,** disminuyendo en un 10% a comparación del periodo anterior. • Los grupos que integran la protección de dispositivos por plataforma, en Microsoft Intune (Endpoint) son los siguientes: - ADD_Dispositivos_472: **62** - ADD_Dispositivos_AdministracionCentral: **681** - AAD_Dispositivos_Personales: **1.426** • Para el Microsoft 365 Defender el puntaje de seguridad quedo en 756,51 puntos de 1.395 puntos, con un porcentaje del 54.23 %. • Para el Microsoft Purview se identificó que el puntaje de cumplimiento está en 56% con 11.518 puntos de 20.292 puntos totales, adicional se cuenta con 43 acciones de mejora en cumplimiento y 556 por cumplir. • Para el Entra ID el puntaje de seguridad se encontró en **73,45%** aumentando en un 4% a comparación del periodo anterior. • En el Azure Site Recovery se llevó a cabo: o La actualización del agente asociado al servidor de configuración ASR-SRV. o Configuración y registro del nuevo Appliance		
9	Prestar el servicio de revisión y análisis del plan de recuperación de desastres según lo descrito en el numeral 2.9 del ANEXO – ESPECIFICACIONES TECNICAS, con el fin de mejorar el plan de recuperación tiempo de respuesta ante incidentes y amenazas de seguridad.	A continuación, se relacionan las actividades más relevantes del periodo: • Se ejecutan actividades y reuniones para la mejora del informe de resultados de la primera prueba de simulación para la vigencia 2024.	N/A	N/A
10	Elaborar, entregar y socializar previa aprobación del supervisor, el plan de trabajo del contrato conforme a lo descrito en el numeral 3 del ANEXO – ESPECIFICACIONES TECNICAS.	Se elaboro el cronograma de actividades para el año 2024 y una proyección para el 2025. El avance del proyecto general va en un 21% - Avance Real de la vigencia 2023: 100%. - En el 2024 se tiene un avance del 41%	Plan Global - ADRES-CTO_868_2023 - 06_06_2024 .mpp	N/A
11	Presentar y disponer durante la ejecución del contrato de un equipo base de proyecto que contemple como mínimo los roles, perfiles y experiencia que se describen en el numeral 4 del ANEXO - ESPECIFICACIONES TECNICAS.	En el desarrollo la sesión de revisión de riesgos del proyecto que se realiza mensualmente en el ítem 11 se da cumplimiento a los roles mínimos solicitado por la ADRES.	GEDO-FR05_Acta de Reunion_V02_20240523 - Riesgos.pdf	N/A
12	Aportar la respectiva certificación y mantener la interacción de centro de operaciones de seguridad con mínimo un (1) organismo de respuesta a incidentes de seguridad, conforme a los descrito en el numeral 5 del ANEXO - ESPECIFICACIONES TECNICAS.	Las certificaciones se encuentran vigentes a la fecha de la revisión del informe de cumplimiento para: • FIRST Indra/Minsait realizo proceso de recertificación de ISO 27001.	• Certificate-sia-cert-2023 • IQNetES-SI-0052-2017_2023-11-07.pdf	N/A
13	Aprovisionar, asegurar y mantener durante la ejecución del contrato, sus instalaciones, equipos y los canales o enlaces de conectividad entre la ADRES y las instalaciones del contratista, con el fin de realizar de manera remota la operación del Centro de Operaciones de Seguridad.	Se continua con los canales de comunicación activos y no se han presentado ninguna eventualidad de estos.	N/A	N/A
14	Prestar el servicio adicional de un experto en seguridad bajo el esquema de trabajo hibrido y en la modalidad 5x8, con el fin de acompañar en la ejecución del plan de remediación o mitigación definido por la Entidad, identificar, optimizar y aplicar configuraciones de seguridad y elaborar procedimientos relacionados con la seguridad de la información.	A continuación, se relacionan las actividades más relevantes del periodo: • Gestión de las vulnerabilidades acumuladas. o Vulnerabilidades Web: Identificadas con nivel de riesgo Alto tres (3) y se mitigaron tres (3). o Vulnerabilidades de infraestructura: Identificadas con nivel de riesgo Crítico treinta y tres (33) y se mitigaron veinticuatro (24); como altas ciento ochenta y dos (182) y se mitigaron ciento treinta y cuatro (134). • Apoyo a la construcción del plan de respuesta a incidentes de ciberseguridad.	N/A	N/A

		• Apoyo a la construcción del formato para la declaración de incidentes de seguridad. • Gestión de dispositivos: o Depuración de los dispositivos duplicados. o Validación de compatibilidad de dispositivos. o Escalamientos mesa de servicio de la ADRES, para remediación de incompatibilidad de los dispositivos. • Asignación de casos a la mesa de servicio • Apoyo en la elaboración del Instructivo: Entrega de credenciales protegidas. • Acompañamiento en el desarrollo del plan de capacitación de Ingeniería social		
15	Prestar el servicio de monitoreo de marca en la modalidad 7x24 por la duración del contrato que incluye: i) un dominio, ii) una (1) marca, iii) filtración de credenciales, iv) monitoreo de abuso de marca (Redes sociales, dominios similares, phising) y v) un (1) informe del servicio por mes.	A continuación, se relacionan las actividades más relevantes del periodo: • En el transcurso del periodo se identificaron **421 eventos**, los cuales están clasificados en 4 tipos: - Fuga de Datos: **75** - Fraudes Digitales: **321** - Piratería Online: **0** - Cybersquatting: **25** • Los tipos de fraude digital identificados son: o Phishing: **224** o Perfil falso en red social: **95** o Aplicación móvil falsa: **2** • Se identificaron **24 dominios** los cuales no alojan contenido que se categorice como malicioso según su criticidad, también se identificó **1 dominio** catalogado como suplantación de información, el cual fue reportado para las pertinentes acciones administrativas.	Monitoreo de Marca y Fuente de Inteligencia de Amenazas_Mayo_2024.docx	N/A
16	Prestar un servicio de inteligencia de amenazas con fuente de datos comercial e incorporación de indicadores de compromisos a Microsoft Sentinel.	Actualmente se encuentra en funcionamiento la herramienta (AXUR) como fuente de inteligencia de amenazas; también se cuenta con (4) reglas de analítica para el análisis y la correlación de eventos en el SIEM – Sentinel.	N/A	N/A

Hago constar que durante el periodo reportado se adelantaron las anteriores obligaciones y/o actividades.

JOSE FERNANDO QUINTERO VARGAS

Firmado digitalmente por JOSE FERNANDO QUINTERO VARGAS
Fecha: 2024.06.13 14:30:42 -05'00'

Firma del Contratista

BALANCE ECONÓMICO

Valor Total Contrato (Inicial + Adición)		Valor Pagado	Valor a Pagar	Saldo Liberado	Saldo por Pagar
Vigencia 2023	$ 1,762,183,892.00	$ 1,451,749,187.00	$ 0.00	$ 310,434,705.00	$ 0.00
Vigencia 2024	$ 2,390,471,762.00	$ 585,123,119.00	$ 125,657,574.00	$ 0.00	$ 1,679,691,069.00
Vigencia 2025	$ 2,390,471,762.00	$ 0.00	$ 0.00	$ 0.00	$ 2,390,471,762.00
TOTAL	$ 6,543,127,416.00	$ 2,036,872,306.00	$ 125,657,574.00	$ 310,434,705.00	$ 4,070,162,831.00

La ADRES cancelará al CONTRATISTA, la suma de Ciento veinticinco millones seiscientos cincuenta y siete mil quinientos setenta y cuatro pesos ($125’657.574,00)

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
INDRA Colombia
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	77617130	$ 851’275.300	01/06/2024	30/06/2024	05/06/2024
PENSION	77617130	$ 2.497’989.100	01/05/2024	31/05/2024	05/06/2024
ARL	77617130	$ 142’775.000	01/05/2024	31/05/2024	05/06/2024

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
DEXTERA
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	9467587590	$ 20’889.400	01/05/2024	31/05/2024	23/05/2024
PENSION	9467587590	$ 75’820.700	01/04/2024	30/04/2024	23/05/2024
ARL	9467587590	$ 23’840.900	01/04/2024	30/04/2024	23/05/2024

El Contratista tiene otros Contratos de Prestación de Servicios:

SI ☐ NO ☒

En la eventualidad que la Supervisión verifique que la información suministrada por el Contratista no es consistente o carece de validez, ésta deberá indicar las acciones tomadas: Realizar una breve descripción del hallazgo (Adjuntar soportes)

INFORME PARCIAL DE SUPERVISIÓN

De conformidad con el seguimiento a la ejecución del contrato, el (los) supervisor (es) certifica(n) que:

- El (la) Contratista durante el mes de mayo del 2024, desarrolló y cumplió con el objeto contractual, las obligaciones generales y específicas, presentó y entregó los productos y/o informes establecidos en el Contrato o Convenio en mención.
- Apruebo los informes, productos y demás documentos presentados y entregados por el (la) Contratista durante el periodo mencionado en desarrollo de las obligaciones pactadas en el Contrato o Convenio en mención:
  - Informe mensual del servicio de monitoreo y correlación de eventos de seguridad. i) Monitoreo y Correlación de eventos de Seguridad_Mayo_2024.docx; Anexos: i) SecurityIncident_by_Events.csv, ii) SecurityIncident_by_IncidentNumber.csv
  - Informe mensual del servicio de gestión de incidentes, el cual comprende los reportes i) Matriz de eventos o incidentes de seguridad - Mayo 2024.xlsx
  - Informe mensual del servicio de gestión de infraestructura de seguridad. i) Gestión de infraestructura de seguridad Mayo 2024.docx
  - Informe del servicio Monitoreo y supervisión de actividad de bases de datos, se entregan los siguientes documentos: i) Informe Monitoreo y supervisión de actividad de bases de datos_Mayo_2024.docx ; Anexo: i) Inventario BD.xlsx
  - Informe mensual Monitoreo de Marca y Fuente de Inteligencia de Amenazas: i) Monitoreo de Marca y Fuente de Inteligencia de Amenazas_Mayo_2024.docx
- A la fecha no existen causales de incumplimiento de las obligaciones contractuales que demanden actuaciones conminatorias o sancionatorias por parte de la Administración.
- Verifique la matriz de riesgos del contrato y se estableció, que no se ha materializado ninguno de los riesgos.
- Dejo constancia que el contratista entrego los documentos relacionados, pero por razones de confidencialidad de la información los archivos quedan almacenados en repositorio de Teams denominado Ciberseguridad en la carpeta \Contratos\ADRES-CTO-868-2023 - SOC\3. Ejecución\2. Obligaciones

OBSERVACIONES	
ANEXOS	1. Comprobante del pago de los Aportes respectivos al Sistema de Seguridad Social Integral en Salud y Pensiones y/o Aportes Parafiscales por parte del Contratista. 2. Soportes contractuales cargados en la sección 7 del contrato electrónico (Formato comprimido). 3. Cuenta de cobro o factura, según el Régimen sea Simplificado o Común.

En constancia, firmo:

BENITEZ RODRIGUEZ GUILLERMO MANUEL

Firmado digitalmente por BENITEZ RODRIGUEZ GUILLERMO MANUEL
Fecha: 2024.06.12 08:43:15 -05'00'

Supervisor(es) / Interventor(es)

En constancia, el presente documento se entiende aprobado por las partes una vez el usuario supervisor del contrato efectué la aprobación respectiva en la plataforma de SECOP II.

Lugar y Fecha: Bogotá, D. C.,

[i] Incluir las obligaciones específicas pactadas en el Contrato y/o Convenio.